Privacy Journal

AN INDEPENDENT MONTHLY ON PRIVACY IN A COMPUTER AGE

PO Box 28577
Providence RI 02908

October 2007 Volume 33, Number 12

Scary Stuff

(about pervasive surveillance)

As the government officials responsible for enforcing privacy laws worldwide met last month, there was little of the traditional talk about the nuts and bolts of data protection like opt-in, transparency, or transborder data flows.

Instead, there were urgent and distressed discussions about "uberveillance," "ambient technology," "ubiquitous computing," "ingestible bugs," and nanotechnology. The terms may be overlapping and may in fact be somewhat synonymous. They all refer to an environment in which electronic media are everywhere, gathering and processing information in a seamless way, beyond the control of each human being. The discussions began a few years ago with recognition of a coming "Internet of things," much as public awareness of the Internet began in the 1980s with talk of an "information super highway."

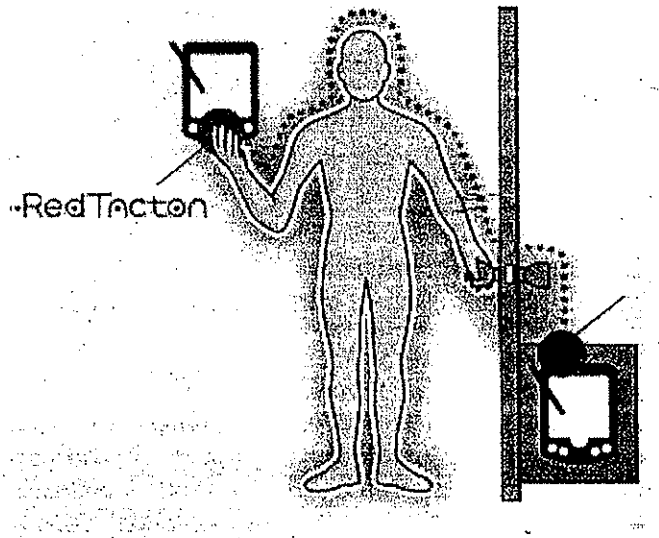
This concern about pervasive informational and locational data processing dominated the discussions at the 29th annual International Conference of Data Protection and Privacy Commissioners in Montreal.

In many ways, Canadian Commissioner Jennifer Stoddart, as host, set up the meeting for this to happen by scheduling an ambitious agenda of futurists and cyber-theorists to educate the commissioners about the new technologies.

Canada Leading the Way

One prime speaker, Ian Kerr, Canada Research Chair in Ethics, Law and Technology at the University of Ottawa, commended Stoddart "for making Canada a leader in academic study of privacy and ubiquitous computing."

Kerr noted that the Canadian Supreme Court had established a hierarchy of privacy values: ***bodily or personal privacy*** (highest level of protection), ***territorial privacy***, and ***informational privacy*** (with a lower level of legal protections under the constitution). In its 2004 ***Tessling*** decision, the Canadian high court "smudged" the three distinctions, Kerr said, by rejecting a lower court's finding that the government's use of ***forward looking infra-red*** (FLIR) technology to detect marijuana cultivation in a home was a search worthy of the highest protection of individual rights.



Instead the high court said that the technology was collecting ***information*** from outside the premises and was legal as conducted. (Under the U.S. Supreme Court's 2001 ***Kyllo*** decision, a warrant would generally be required in this country.)

The technology, as well as the law, has "smudged" the traditional hierarchy, said Kerr. He cited as evidence new ***human-area networking*** technology [above] that permits the human body to be the conduit for electronic transmissions – of information, instructions, behavior and a lot more. See www.redtacton.com.

Kerr was not finished. He said that enhancements of current Internet provider (IP) addresses will soon permit a worldwide total of Web add-

(Continued on page five)

ISSN 0145-7659

Montreal (Continued from page one)

resses to reach 3.4×10^{28} – seven for each atom of every human being. "Thus, we are entering a new era in privacy," he concluded. "Current concepts of consent will not be adequate for this."

While the audience was still agape, Stephanie Perrin, director of Integrity Policy at Service Canada, a co-panelist with Kerr, cited Eastman-Kodak's announcement this year that it has developed an RFID identifying chip that may be swallowed by humans – an ***ingestible bug.*** The patent filing suggested potential uses, including monitoring "bodily events," tracking how a person's digestive track is absorbing medicine, or verifying how a specific medicine is interacting with other drugs in one's body. The RFID tag would disintegrate eventually, the company said.

Peter Hustinx, European Data Protection Supervisor appointed by the European Parliament, suggested from the audience that these same all-encompassing technologies could be the source of new rights and responsibilities for humans. In separate sessions, Alexander Dix, Commissioner for Data Protection for the jurisdiction of Berlin in Germany, used the terms ***ubiquitous computing*** and ***pervasive or invasive computing***. He said that ***ambient intelligence*** is an even greater challenge to European privacy enforcers than terrorism. Ambient intelligence refers to an environment in which electronic de vices support human beings in their daily activities in a way that conceals the computers' in-

ner workings. This will involve embedding devices inside the body, customizing them to the individual, and anticipating needs of the individual.

In still another session, Michael G. Michael, a theologian and technology historian at the University of Wollongong, in New South Wales, Australia, warned that ***uberveillance***, a term he is said to have created, will lead to increased cases of insanity and mental distress. "Mental illness will become an increasingly confronting factor as these issues develop," he frowned.

Another threatening term often used in these contexts is ***nanotechnogy***, which refers to a miniaturization of technology allowing applications originally deemed impossible. Still another term is ***biobanking***, which, in the words of an IBM developer, "aims to empower researchers

with unprecedented access to critical molecular and clinical information to accelerate a more personalized paradigm of medicine. Biobanks – sometimes called biorepositories or tissue banks – are a critical resource for Twenty-First Century clinical research and medicine because they naturally generate lots of genotypic and phenotypic data. Combining the wealth of genetic and molecular information now emerging with patient records and other clinical records will help researchers understand disease at the molecular level, ultimately leading to innovative new personalized therapies and treatments."

Even – especially– children are already subjects of this pervasive monitoring, according to a session on Web sites that prey on children. Sites like neopets.com, webkinz.com, survey smash.com, and Barbie.com manipulate children by offering bonus points for loyalty to products and to the site. Children are coerced into visiting on a regular basis. They are forced to give care, love, and attention to fictional characters and animals. Collecting information on child-oriented Web sites is regulated by American law (even though kids, of course, have little difficulty circumventing the parental consent rules), but manipulating children online is not regulated.

The American presence at the meeting of data protection commissioners was largely limited to the keynote speaker, Homeland Security Chief Michael Chertoff, who began the conference with a plea to recognize the need for strong national security precautions. A few representatives of non-profit organizations in the U.S. spoke at the conference, but the U.S. role – always minimal – was even more minimal than usual.